Implementasi Kriptografi Dengan Enkripsi *Shift Vigenere Chiper* Serta *Checksum* Menggunakan CRC32 Pada Data Text

Syaiful Anwar[1], Indra Nugroho[2], Asep Ahmadi[3]

[1]*Divisi IT, PT Bank Pundi Indonesia*
Jl. RS. Fatmawati No. 12 Jakarta 1214 Indonesia
[1]aefsyaiful.anwar@gmail.com
[2,3]*Jurusan Magister Ilmu Komputer, Universitas Budi Luhur*
Jl. Ciledug Raya Petukangan Utara Jakarta 12260 Indonesia
[2]indnugrohoo@gmail.com
[3]asep.ahmadibl@gmail.com

Abstrak - **Kemajuan teknologi di bidang komputer dan telekomunikasi berkembang sangat pesat. Lalu lintas pengiriman data dan informasi yang semakin global, serta konsep open system dari suatu jaringan memudahkan seseorang untuk masuk ke dalam jaringan tersebut. Hal tersebut dapat membuat proses pengiriman data menjadi tidak aman dan dapat saja dimanfaatkan oleh pihak lain yang tidak bertanggung jawab, yang mengambil informasi atau data yang dikirimkan tersebut di tengah perjalanan. Maka dibutuhkan suatu sistem keamanan yang dapat menjaga kerahasiaan suatu data, sehingga data tersebut dapat dikirimkan dengan aman. Salah satu solusi untuk menjaga keamanan dan kerahasiaan pada proses pengiriman data dengan menggunakan teknik kriptografi. Dalam makalah ini penulis merealisasikan suatu perangkat lunak enkripsi dan dekripsi teks sebagai implementasi dengan menggunakan enkripsi Shift Vigenere Chiper. Di samping itu untuk meningkatkan keamanan pada perangkat lunak disertakan juga proses Checksum, sehingga perangkat lunak dapat mendeteksi adanya perubahan data atau informasi yang dikirimkan serta menjamin keaslian pengirim informasi dengan menggunakan CRC32.**

Kata Kunci : ***enkripsi, Vigenere, Checksum, CRC32***

I. PENDAHULUAN

Jaringan komputer dan internet telah mengalami perkembangan yang sangat pesat. Teknologi ini mampu menghubungkan hampir semua komputer yang ada di dunia sehingga dapat saling berkomunikasi dan bertukar informasi berupa data teks seperti data keuangan, data user name dan password dari account suatu perusahaan, gambar bergerak suara maupun email. Seiring dengan perkembangan tersebut, secara langsung ikut mempengaruhi cara berkomunikasi. Jika dahulu untuk berkomunikasi pesan atau surat dengan menggunakan pos, sekarang telah banyak layanan e_mail di internet yang dapat mengirimkan pesan secara langsung kepenerimanya. Akan tetapi sebagai suatu jaringan publik, internet rawan sekali terhadap pencurian data. Maka salah satu cara untuk melindungi data dengan menggunakan seni Kriptografi.

Oleh sebab itu dengan permasalahan yang ada, maka dibutuhkanlah pengamanan data untuk menjaga kerahasiaan dengan komposisi kejahatan dunia maya yang semakin luas.

II. LANDASAN TEORI

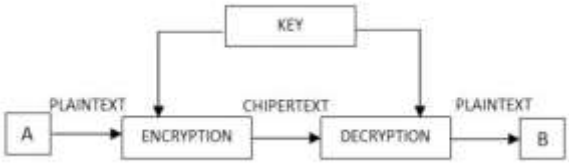
A. *Kriptografi*

Secara bahasa Kriptografi berasal dari kata crypto yang berarti rahasia dan graphy yang berarti tulisan. Jadi kriptografi dapat diartikan sebagai tulisan rahasia. Secara istilah dapat didefinisikan sebagai studi tentang teknik-teknik matematika yang berhubungan dengan keamanan informasi. Teknik kriptografi terdiri dari simetri dan asimetri. Teknik ini digunakan untuk mengamankan aplikasi (kemanan informasi) sehingga dapat menjaga kerahasiaan, integritas data, autentikasi data dan *non-repudiation*[1].

Kriptografi diperlukan karena pada dasarnya informasi sangat penting bagi segala aspek, tuntutan kemanan informasi berubah dari waktu ke waktu. Perubahan tuntutan ini terjadi karena transformasi atau penggunaan perlengkapan kebutuhan utama untuk pertukaran informasi, dari mulai cara tradisional (fisik) yang membutuhkan mekansime pengarsipan atau administrasi secara fisik dan membutuhkan ruang yang lebih besar, menggunakan otomatisasi komputer personal, sampai transfer informasi melalui penggunaan jaringan komputer, baik intranet maupun internet yang sekarang menjadi tren dan kebutuhan.

Kriptografi secara umum merupakan ilmu dan seni untuk menjaga kerahasian berita [2]. Kriptografi juga dapat diartikan sebagai ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi. seperti kerahasiaan data, keabsahan data, integritas data, serta Otentikasi data [2]. Namun, pada kriptografi tidak semua aspek keamanan informasi akan ditangani.

Kriptografi memiliki dua konsep utama, yaitu enkripsi (encryption) dan dekripsi (decryption). Enkripsi adalah proses penyandian plainteks menjadi cipherteks, sedangkan dekripsi adalah proses mengembalikan cipherteks menjadi plainteks semula. Enkripsi dan dekripsi membutuhkan kunci sebagai parameter yang digunakan untuk transformasi[4].



Gambar 1. Skema enkripsi dan dekripsi kriptografi type symmentric key [4]

Enkripsi dan dekripsi pada umumnya membutuhkan penggunaan sejumlah informasi rahasia, disebut sebagai kunci. Untuk beberapa mekanisme enkripsi, kunci yang sama digunakan baik untuk enkrispi dan dekripsi; untuk mekanisme yang lain, kunci yang digunakan untuk enkripsi dan dekripsi berbeda. Dua tipe dasar dari teknologi kriptografi adalah symmentric key (secret/private key) cryptography dan asymmetric (public key). Pada symmentric key cryptography, baik pengirim maupun penerima memiliki kunci rahasia yang umum. pada asymmentric key cryptography, penerima masing-masing berbagi kunci public dan private. Kriptografi saat ini lebih dari enkripsi dam dekripsi saja.

Ada empat tujuan mendasar dari kriptografi yang juga merupakan aspek keamanan informasi adalah :

1) Kerahasiaan : layanan yang digunakan untuk menjaga isi dari informasi dari siapapun kecuali yang memiliki kunci rahasia atau otoritas untuk membuka informasi yang telah disandikan.

2) Integritas Data : Berhubungan dengan penjagaan dari perubahan data secara tidak sah. Untuk dapat menjaga integritas data, suatu sistem harus memiliki kemampuan untuk mendeteksi manipulasi data yang dilakukan pihak-pihak yang tidak berhak, antara lain penyisipan, penghapusan, dan pendistribusian data lain ke dalam data yang asli.

3) Otentifikasi : Berhubungan dengan identifikasi, baik secara kesatuan sistem maupun informasi itu sendiri. Dua pihak yang saling berkomuniasi harus saling memperkenalkan diri. Informasi yang dikirimkan harus di Otentikasi keasliannya, isi datanya, waktu pengiriman dan lain sebagainya.

4) Non-repudiasi : Merupakan usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman atau terciptanya suatu informasi oleh yang mengirimkan atau membuat.

B. Vigenere

Vigenere Cipher merupakan salah metode kriptografi klasik polyalphabetic. Vegenere cipher ini sendiri sebenarnya merupakan pengembangan dari Caesar cipher [6], dimana jika setiap karakter pada plaintext digeser dengan jumlah pergeseran yang sama, namun pada Vegenere cipher setiap karakter digeser dengan jumlah pergeseran yang berbeda.

Untuk mengenkripsikan plaintext, kita membutuhkan sebuah tabel Vegenere yang berisi alfabet yang dituliskan dalam 26 baris, masing-masing baris digeser satu urutan ke kiri dari baris sebelumnya, membentuk ke-26 kemungkinan Caesar cipher. Setiap huruf disandikan dengan menggunakan baris yang berbeda-beda, sesuai kata kunci yang diulang.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Gambar 2. Tabel Vigenere [3]

Sandi Vigenere berasal dari nama penemunya, Blaise de Vigenere, seorang kriptografer asal Perancis. Walaupun Giovan Batista Belaso telah lebih dahulu menemukan sandi sebelumnya, namun Vigenere berhasil menemukan kunci sandi yang lebih kuat.

Sandi ini dikenal luas selain karena mudah dimengerti dan diimplementasi, untuk para pemula sandi ini sering dirasakan tidak dapat dipecahkan (unbreakable), dimana sandi ini sering disebut le chiffre indéchiffrable (bahasa perancis untuk “tidak dapat dipecahkan”). Pada abad ke-19, banyak orang yang mengira Vigenere adalah penemu sandi ini, sehingga, sandi ini dikenal luas sebagai "Sandi Vigenere"[3].

Misalnya, teks terang yang hendak disandikan adalah perintah "CONANEDO": Sedangkan kata kunci antara pengirim dan tujuan adalah "KEREN", karena ada 8 huruf, maka sandi akan diulang jadi KERENKER, sesuaikan kunci berulang-ulang sesuai dengan jumlah kata yang dimaksud. Pada tabel tersebut, C bertemu dengan K berada di huruf 'M', lalu huruf O bertemu dengan E di huruf 'S', dan seterusnya.

Teks Asli	: CONANEDO
Kata kunci	: KERENKER
Hasil Vigenere	: MSEEAOHF

Jadi, hasil enskripsi Vigenere dari kata “CONAN EDO” dengan menggunakan kata kunci “KEREN” adalah “MSEEAOHF”

Kita dapat membuat sandi Vigenere tanpa menggunakan Tabel Vigenere, dengan menggunakan cara “ Huruf hasil Vigenere = (Huruf Asli dalam bentuk angka) + (Kata Kunci dalam bentuk angka) - 1 “ untuk mengetahui teks hasil Vigenere nya. Jika hasil Vigenere dalam bentuk angka lebih besar daripada 26, maka kurangilah hasil tersebut dengan 26.
Contoh :

Huruf Asli	: C = 3
Huruf Kunci	: K = 11
Huruf hasil Vigenere	: 3 + 11 - 1 = 13 (13 = huruf M)
Huruf Asli	: O = 15
Huruf Kunci	: R = 18
Huruf hasil Vigenere	: 15 + 18 - 1 = 32 (32 - 26 = 6 = huruf F)

1) Shift Vigenere Cipher : Shift Vigenere Cipher secara umum prosesnya sama seperti pada vigenere. Namun pada Shift Vigenere Cipher sudah dilakukan modifikasi dengan mengulang password atau key dengan dilakukan pergeseran karakter pada setiap kali pengulangan. Misal pada plaintext dengan panjang 10 dan key INDRA jika menggunakan vigenere yang umum maka key menjadi INDRAINDRA, akan tetapi jika menggunakan Shift Vigenere maka password-nya akan menjadi INDRAARDNI.

C. Parity Checksum

Checksum merupakan salah satu skema dari Redudancy Check (RC). RC adalah proses pendeteksian dan pengkoreksian error dari sebuah data, ini merupakan solusi untuk melindungi integritas/keaslian dari sebuah data. Biasanya Checksum disimpan dibagian header dari data [6].

Berikut ini Langkah-langkah pencarian dalam mencari nilai Checksum pada sebuah data :

a. Jumlahkan semua byte pada data.
b. Hilangkan carry (Sisa hasil penjumlahan pada bilangan hexa) bila ada.
c. Cari two's complement hasil nomor 2, maka didapatkanlah nilai checksum

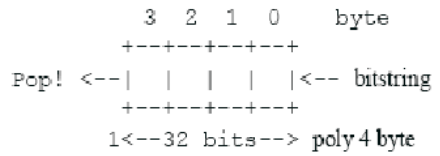
Contoh:

Diberikan 4 byte: 0x15, 0x7F, 0x86, 0x5C

a. 0x15 + 0x7F + 0x86 + 0x5C = 0x176
b. 0x176 ⟶ 0x76
c. Two's complement(0x76) = 0x8A,
d. jadi nilai Checksum = 0X8A

D. CRC 32

CRC 32 adalah metode yang digunakan untuk mendeteksi kesalahan dengan menggunakan polynomial 32 bit atau dengan kata lain polynomial 4 byte[4]. Proses perhitungan



pada CRC 32 bit adalah sebagai berikut:

4 ruang kosong pada ilustrasi di atas menggambarkan register yang akan kita gunakan untuk menampung hasil CRC sementara (pada proses pembagian yang melibatkan operasi XOR). Proses yang dilakukan pada register ini adalah :

a. Masukkan bitstring (data) ke dalam register dari arah kanan ke kiri (shift per byte) setiap saat register tidak terisi penuh.
b. Jika register sudah terisi penuh (berisi 4 byte), maka geser satu byte kearah kiri (keluar register), dan isi register dari arah kanan dengan 1 byte dari bitstring.
c. Jika register yang digeser keluar punya nilai 1, maka lakukan operasi XOR terhadap keseluruhan isi reister (termasuk yang telah digeser keluar, dimulai dari bit tertinggi yang bernilai 1) dan nilai dari poly. Ulangi langkah ini sampai semua bit dari byte yang tergeser keluar bernilai 0.
d. Ulangi langkah 2 dan 3 sampai semua proses bitstring (data inputan) selesai diproses. Pada CRC 32, untuk setiap byte yang digeser keluar dapat dihitung nilainya yang digunakan dalam operasi XOR dengan isi register. Nilai – nilai yang tersimpan di dalam register disebut dengan table CRC.

Proses dalam validasi digunakan CRC cek. Pada CRC cek, pertama kali akan dilakukan inisialisasi tabel kemudian iCRC diatur sehingga semua bit-nya bernilai satu.

Tabel CRC terdiri dari 256 buah nilai yang tiap nilainya mewakili satu karakter. Nilai ini dibuat secara acak, yang masing-masing memiliki panjang 64 bit. Setiap karakter pada teks diubah dalam kode ASCII kemudian di XOR dengan iCRC yang sebelumnya telah di AND dengan bilangan heksa FF, hasilnya akan menjadi indeks untuk table CRC. Keluaran dari table di XOR dengan iCRC yang telah digeser ke kanan sebanyak delapan bit dan hasilnya menjadi iCRC yang baru, kemudian karakter berikutnya akan diproses. Setelah semua karakter selesai diproses, iCRC di XOR dengan bilangan heksa FFFFFFFF menjadi CRC [6], terlihat pada gambar 3.

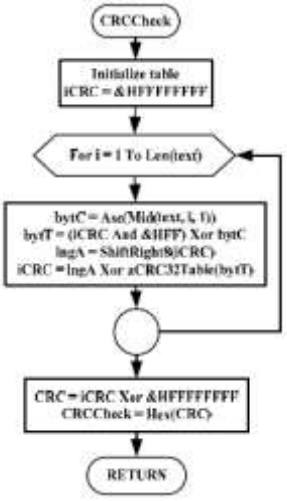
Gambar 3. Diagram Alur CRCCheck

E. Java

Java lahir pada saat penelitian yang dilakukan oleh sejumlah insinyur di sun California pada tahun 1991[3]. Mereka membuat proyek pembuatan bahasa pemrograman yang dapat berjalan pada perangkat yang memiliki memori ukuran kecil. Selain itu mereka juga menginginkan progam dapat berjalan di platform mana pun, ini dikarenakan setiap perangkat mempunyai manufaktur yang berbeda. Pada mulanya, mereka menamakan proyek ini dengan nama "Green Project". Berikut keunggulan Java :

1) Sederhana : Bahasa pemrograman java menggunakan sintaks mirip dengan C++ namun sintaks pada java telah banyak diperbaiki terutama menghilangkan penggunaan

ISSN: 2406-7768



pointer yang rumit dan multiple inheritance. Java juga menggunakan automatic memory allocation dan memory garbage collection.

2) Berorientasi objek : Java menggunakan pemrograman berorientasi objek yang membuat program dapat dibuat secara modular dan dapat dipergunakan kembali.

3) Dapat didistribusikan dengan mudah : Java dibuat untuk membuat aplikasi terdistribusi secara mudah dengan adanya libraries networking yang terintegrasi.

4) Interpreter : Program java dijalankan menggunakan interpreter yaitu Java Virtual Machine (JIT). Hal ini menyebabkan kode sumber java yang telah dikompilasi menjadi bytecode java dapat dijalankan pada platform yang berbeda-beda.

5) Robust : Java mempunyai reliabilitas yang tinggi. Kompilator pada java mempunyai kemampuan mendeteksi eror secara lebih teliti dibandingkan bahasa pemrograman lain.

6) Aman : Sebagai bahasa pemrograman untuk aplikasi internet dan terdistribusi, java memiliki beberapa mekanisme keamanan untuk menjaga aplikasi agar tidak digunakan untuk merusak system computer yang menjalankan aplikasi tersebut.

7) Arsitektur Netral : Program java bersifat platform independent. Program cukup mempunyai satu buah versi yang dapat dijalankan pada platform yang berbeda dengan Java Virtual Machine.

8) Portable : Kode sumber maupun program java dapat dengan mudah dibawa le platform yang berbeda beda tanpa harus dikompilasi ulang.

9) Kinerja : Kinerja pada java sering dikatakan kurang tinggi. Namun kinerja java dapat ditingkatkan menggunakan kompilasi java lain seperti buatan Inprise, Microsof, ataupun Symantec yang menggunakan Just in Time Compilers(JIT).

10) Dinamis : Java didesain untuk dapat dijalankan pada lingkunga yang dinamis. Perubahan pada suatu kelas(class) dengan menambahkan property ataupun method dapat dilakukan tanpa mengganggu program yang menggunakan kelas tersebut.

11) Multithreated : Java mempunyai kemampuan untuk membuat suatu program yang dapat melakukan beberapa pekerjaan sekaligus dan simultan.

III. ANALISA

A. Analisa Masalah

Kriptografi adalah ilmu pengetahuan dan seni menjaga pesan agar tetap aman[5]. Kriptografi memiliki dua konsep utama, yaitu enkripsi (encryption) dan dekripsi (decryption). Enkripsi adalah proses penyandian plainteks menjadi cipherteks, sedangkan dekripsi adalah proses mengembalikan cipherteks menjadi plainteks semula. Enkripsi dan dekripsi membutuhkan kunci sebagai parameter yang digunakan untuk transformasi.

Oleh karena itu dibutuhkan aplikasi untuk dapat menyembunyikan informasi dengan memiliki keamanan ganda serta masih layak/utuh atau ada tidaknya informasi dari file gambar yang ditransfer tersebut dilihat.

B. Penyelesaian Masalah

Dalam penyelesaian masalah yang dianalisa sebelumnya secara garis besar akan dilakukan tahapan penyelesaian dengan cara :

a. Menyisipkan pesan/text
b. Menggunakan pattern (pola) pada hidden text
c. Menggunakan password untuk security
d. Menggunakan CheckSum untuk error detection
e. Encoding dan Decoding file

C. Program Aplikasi

1) Analisa Aplikasi Usulan : Untuk memperkuat kerahasiaan dari suatu pesan maka digunakan Kriptografi. Ada berbagai macam metode dalam Kriptografi, salah satunya adalah Shift Vigenere Cipher, dengan metode ini dibutuhkan sebuah key dalam melakukan enkripsi dan dekripsi. Pada enkripsi atau dekripsi menggunakan Vigenere jika panjang plaintext lebih besar dari panjang key maka key akan diulang, oleh karena itu untuk mempersulit kriptanalis untuk melakukan dekripsi dari ciphertext dilakukan modifikasi Vigenere dengan melakukan pergeseran pada key pada setiap pengulangan key ketika proses enkripsi atau dekripsi dan disebut dengan Shift Vigenere.

Aplikasi nantinya harus dapat mengetahui apakah text yang akan di-decode merupakan hasil encode dari aplikasi ini atau bukan. Aplikasi juga harus dapat mendeteksi password yang dimasukkan untuk melakukan decode apakah sama dengan password yang digunakan pada saat melakukan encode file. Dan jika telah terjadi perubahan data oleh orang lain atau karena terjadi editing pesan maka aplikasi dapat mendeteksi dan memberikan informasi kepada user bahwa data sudah berubah dengan menghitung nilai CheckSum dari pesan. Untuk menangani hal tersebut maka kita harus membuat sebuah pattern (pola) pada hidden text.

2) Metode Kerja Aplikasi Usulan: Langkah awal untuk melakukan adalah enkripsi. Metode yang digunakan dalam melakukan enkripsi adalah shift vigenere cipher, sama seperti vigenere pada umumnya akan tetapi pada shift vigenere dilakukan pergeseran tiap karakter key-nya pada setiap pengulangan yang terjadi.

Setelah melakukan enkripsi pada pesan, kemudian hitung nilai checksum dan ubah menjadi CRC32. Dari proses checksum tersebut maka kita sudah memiliki hidden text yang berupa kode unik yang telah di password.

Nilai CRC32 dihitung dan digabungkan sebelum dilakukan transmisi data atau penyimpanan, dan kemudian penerima akan melakukan verifikasi apakah data yang diterima tidak mengalami perubahan ataupun kerusakan. CRC32 juga melambangkan panjang checksum dalam bit. Bentuk CRC32 yang disediakan untuk algoritma sesuai dengan ide pembagian ”polynomial”. Dan hal ini digunakan untuk memperhitungkan checksum yang sama dari seluruh algoritma CRC32.

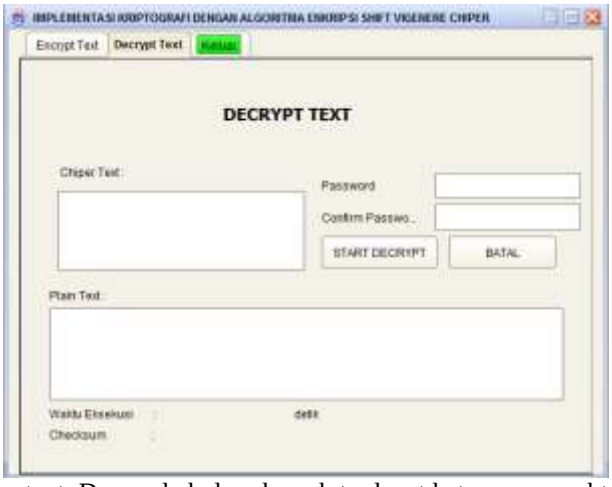
Banyak bermunculan software-software jahat dan juga perkembangan virus computer yang semakin canggih membuat metode Checksum CRC32 lantas digunakan untuk mengetahui mendeteksi virus dengan acuan nilai CRC32-nya. Nilai CRC32 adalah nilai yang didapat dari besar file dan nama file yang dibandingkan dengan tabel CRC32 yang sudah ada acuannya.

D. Rancangan layar

1) Rancangan Layar Encode File : Sebelum aplikasi dibuat, diperlukan rancangan layar yang disesuaikan dengan kebutuhan user. Karena rancangan layar merupakan salah satu komponen penting untuk sebuah program, maka desain dibuat sangat sederhana untuk memudahkan user dalam menjalankan program tersebut

Gambar 4. Perancangan Design antarmuka encrypt

Pada tampilan diatas penulis membuat perancangan yg user friendly agar user mudah untuk memahaminya. Yang dimana pada kolom plain text user memasukan pesan rahasia yang akan di kirimkan kepada yg di tuju guna terjaga kerahasiannya. Sebelum pesan di encrypt maka user memasukan password untuk keamanan pada pesan yang akan di encrypt. Maka barulah pada tombol start encrypt pesan akan diubah menjadi chipper text yang akan tampil di kolom



chiper text. Dan pada kolom bawah terdapat keterangan waktu eksekusi dan checksum dari sebuah program yang akan di tampilkan.

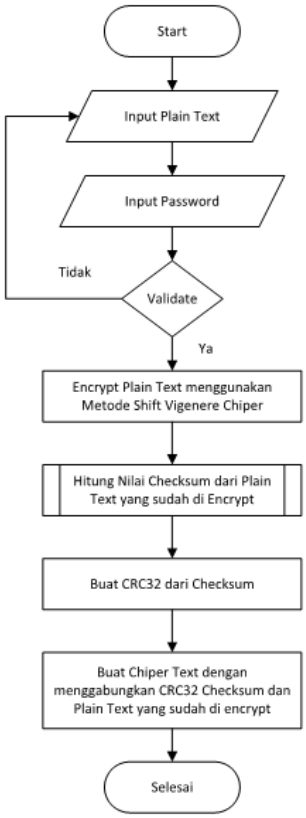
2) Rancangan Layar Decode File : Pada perancangan dibawah, pada kolom chiper text yang di hasilkan dari encrypt data di masukan dan barulah password di masukan sesuai password yang di buat. Maka akan muncul plain text yang telah di buat. Dan pada keterangan di bawah mengenai waktu dan checksum akan di informasikan berapa lama waktu yang di perlukan untuk mengeksekusi sebuah pesan dan hasil code checksumnya.

Gambar 5. Perancangan Design antarmuka Decrypt

E. Flowchart

Di dalam menggambarkan urutan proses pada aplikasi ini, akan digunakan flowchart untuk memperjelas aliran proses. Di bawah ini akan digambarkan beberapa flowchart untuk masing-masing proses.

1) Flowchart Enkripsi File : Flowchart berikut merupakan gambaran alur proses Encode File, form ini terdapat fasilitas proses menyembunyikan pesan. Urutan proses yang akan dilalui pada Enkripsi File digambarkan dengan Flowchart berikut ini:

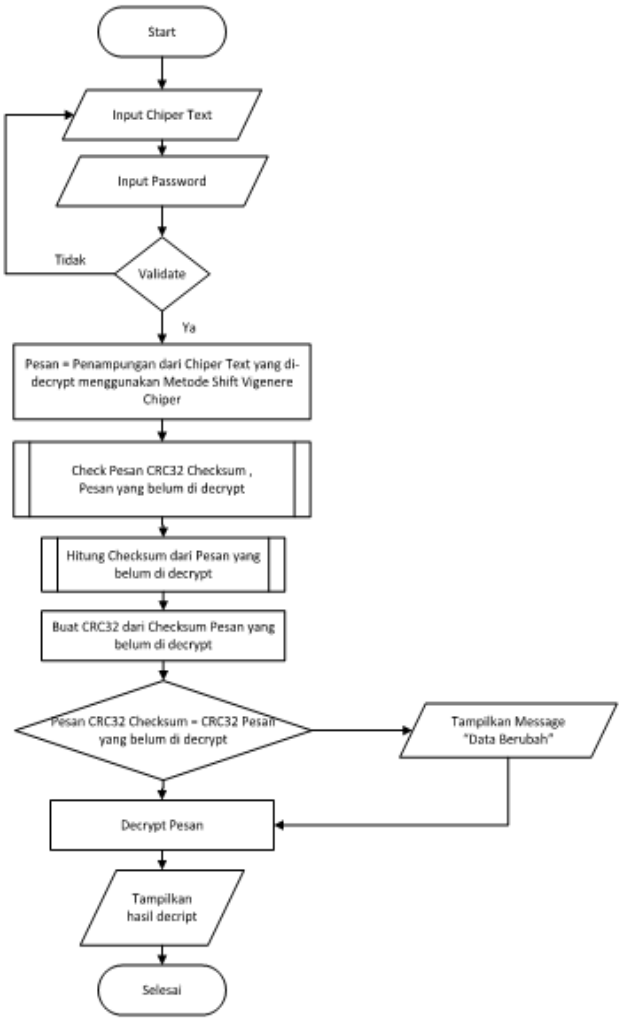


Gambar 6. Flowchart Enkripsi Text

Proses Enkripsi sebagai berikut :

a. Masukan teks atau buka plainteks dan masukan Kunci.
b. Baca semua kunci yang telah dimasukan
c. setelah penginputan password maka akan di validasi password apabila belum sesuai makan akan kembali pada penginputan plain text
d. Setelah di validasi pesan akan di encrypt menggunakan metodes Shift Vigenere Chiper
e. Selelah itu akan di hitung nilai checksum dari plain text yang sudah di enkripsi
f. setelah itu akan di buat CRC32 dari checksum
g. Buat chiper text dengan menggabungkan CRC32 Checksum dan plain text yang sudah di enkripsi.
h. Proses Selesai.

2) Flowchart Dekripsi File : Flowchart berikut merupakan gambaran alur proses Decode File, form ini terdapat fasilitas proses menampilkan pesan yang tersembunyi pada file yang sudah di-enkripsi. Urutan proses yang akan dilalui pada dekripsi File digambarkan dengan Flowchart berikut ini:



Gambar 7. Flowchart Dekripsi File

Proses Dekripsi sebagai berikut :

a. Masukan Chiper Text yang telah dihasilkan proses enkripsi.
b. Masukan Passwoord yang telah dibuat.
c. Password akan divalidasi, apabila password salah akan kembali pada penginputan chipert text
d. setelah di validasi pesan chiper text yang di dekrip menggunakan metode shift Vigenere Chiper
e. Dilakukan pengecheckan pesan CRC32 Checksum pesan yang belum di dekrip
f. Akan di hitung Checksum dari pesan yang belum di dekrip
g. Pesan CRC32 yang belum di dekrip akan di tampilkan dengan pesan data berubah apabila ada yang berubah
h. Apabila sesuai makan pesan akan di dekripsi
i. Akan di tampilkan pesan dekripsi.
j. Proses selesai

IV. IMPLEMENTASI DAN ANALISA HASIL UJI COBA

A. Spesifikasi Hardware dan Software

Di bawah ini merupakan minimum spesifikasi hardware (perangkat keras) dan software yang mendukung dalam pengoperasian aplikasi steganografi.

1) Hardware

- PC Pentium Core 2 duo (2.0 GHz)
- RAM / Memori 2 GB
- Keyboard dan Mouse
- Monitor
- Hardisk 160 GB

2) Software

- Sistem Operasi Windows 7.
- Java Runtime Environment 1.7.0.21 (JRE 7 Update 21)

B. Implementasi Program

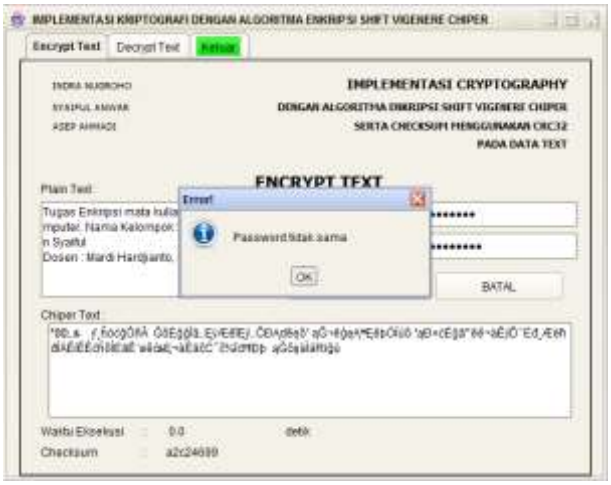
Implementasi program berguna untuk mengetahui apakah program yang telah dibuat dapat berjalan secara maksimal atau bahkan terjadi kesalahan-kesalahan yang tidak diinginkan, maka dari itu program tersebut harus diuji terlebih dahulu mengenai kemampuannya agar dapat berjalan sesuai dengan yang diharapkan pada saat implementasi nantinya. Berikut ini adalah tampilan program beserta penjelasan penggunaan program di masing-masing tampilan program.

1) Tampilan Layar Enkripsi Text : Pada aplikasi ini pada saat pertama kali kita menjalankan program maka akan langsung menuju ke form Encode File. Ada 2 tab menu pada aplikasi ini yaitu menu Encrypt Text dan Decrypt text. Pada Form Encrypt Text pengguna dapat melakukan enkripsi text. Caranya pengguna mengisi pesan yang akan di enkripsi, kemudian mengisi password dan confirm password untuk melakukan enkripsi maupun dekripsi. Password harus berisi huruf dan angka serta memiliki panjang minimal 8 karakter.

a. Melakukan Enkripsi Text

Gambar 8. Implementasi Enkripsi

b. Melakukan Enkripsi Text dengan menggunakan Password yang tidak sama.

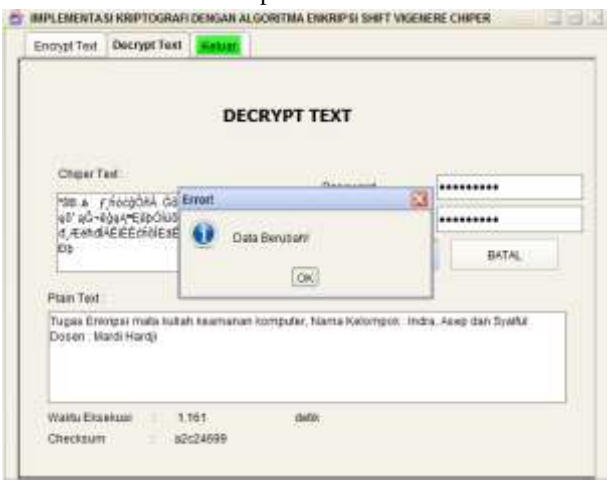


Gambar 9. Implementasi Enkripsi dengan password yang tidak sama

2) Tampilan Layar Dekripsi Text : Pada Form Dekripsi Text pengguna dapat melakukan Dekripsi Text dari text yang di-enkrip dengan menggunakan aplikasi ini. Proses Dekripsi Text dilakukan untuk mendapatkan pesan yang tersimpan dalam aplikasi. Caranya pengguna memilih menu Decrypt untuk dilakukan dekripsi, kemudian copy chiper text setelah itu mengisi password yang sama pada saat melakukan enkripsi.

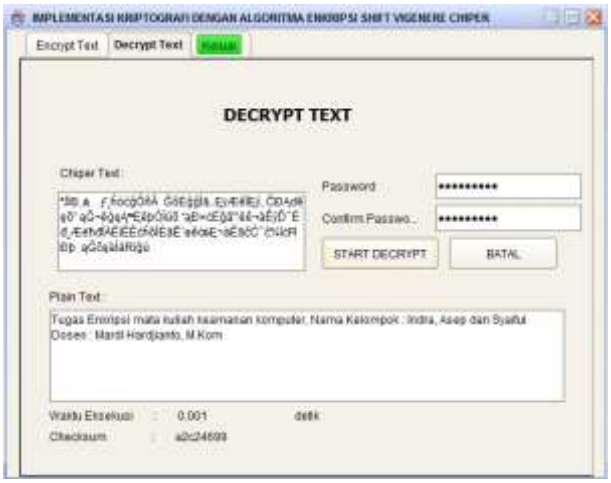
Pada saat proses dekripsi aplikasi sudah dapat mendeteksi apakah text sudah di-enkripsi dari aplikasi ini, dan mencocokan apakah password yang digunakan pada saat melakukan dekripsi sama pada saat melakukan enkripsi. Serta aplikasi juga telah dapat mendeteksi jika pesan sudah mengalami perubahan, karena kemungkinan pesan diubah oleh orang lain atau karena proses edit text.

a. Melakukan Deskripsi



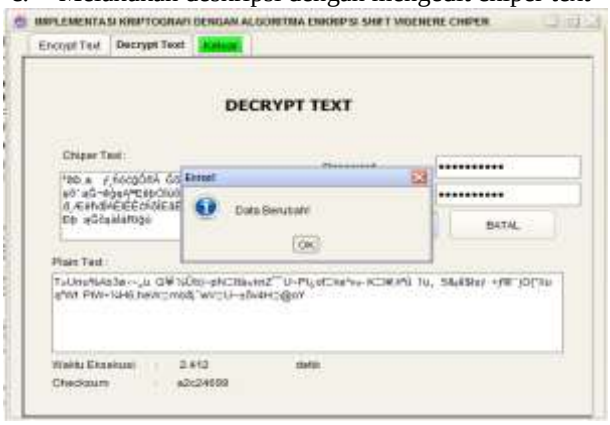
Gambar 10. Implementasi Deskripsi

b. Melakukan Deskripsi dengan password yang salah



Gambar 11. Implementasi Deskripsi dengan password yang salah

c. Melakukan deskripsi dengan mengedit chiper text



Gambar 12. Implementasi Deskripsi dengan merubah isi chiper text.

3) Evaluasi Program : Dan dalam evaluasi tersebut ditemukan beberapa kelebihan dan kekurangan program yang dilihat dari beberapa kondisi dan situasi. Adapun kelebihan dan kekurangan pada aplikasi yang dikembangkan adalah sebagai berikut:

Kelebihan

a. Program dapat dengan mudah dioperasikan oleh pengguna, karena memiliki user interface (tampilan antar muka) yang baik dan user friendly.
b. Dapat dioperasikan di komputer yang memiliki spesifikasi rendah karena program aplikasi ringan ketika dijalankan.
c. Integritas data dari Text tetap dapat terjaga, karena diimplementasikan dengan keamanan berganda, yaitu dengan enkripsi dan pattern atau pola pada hidden text.
d. Pada saat melakukan dekripsi aplikasi dapat mendeteksi text yang di-enkripsi dari aplikasi ini atau bukan.
e. Aplikasi dapat mendeteksi bahwa password yang digunakan dalam melakukan deskripsi apakah sama seperti pada saat melakukan enkripsi.
f. Aplikasi dapat mendeteksi jika terjadi perubahan pada hididen text.

Kekurangan

a. File yang bisa disisipkan hanya Text
b. Belum ada tombol clear data.
c. Aplikasi masih sangat sederhana, hanya menampilkan keunggulan dari sebuah metode pengamanan.
d. Pesan yg di enkripsi tidak ada tombol copy atau salin.

V. KESIMPULAN

Beberapa kesimpulan yang diperoleh dari perancangan program aplikasi ini adalah sebagai berikut.

a. Berhasil dikembangkan program aplikasi kriptografi untuk pengamanan baik pesan maupun file. Kebutuhan fungsional dari program aplikasi, seperti proses enkripsi dan error checking, serta penggunaan kunci (key) sudah dapat dilakukan dengan benar.
b. Berhasil melakukan enkripsi pada text.
c. Program aplikasi kriptografi ini membatasi akses dari orang yang tidak berhak atas pesan atau data rahasia.
d. Program ini berhasil dalam menyisipkan dan mengekstrasi pesan atau data rahasia dengan sempurna, karena pesan yang diekstraksi sama dengan pesan yang disisipkan, tidak merubah sedikitpun text atau adanya perubahan dalam text tersebut.

VI. DAFTAR PUSTAKA

[1] R. Munir, Kriptografi, Bandung: Informatika Bandung, 2006.

[2] S. A. Vanstone, C. P. van Oorschot and A. J. Menezes, Handbook Of Applied Cryptography, Massachusetts: Massachusetts Institute of Technology , 1996.

[3] A. P. H, T. P. Rahayu, Yakub and Hariyanto, "Jurnal Informatika. Jurusan Teknik Informatika. STMIK Dharma Putra Tangerang," Implementasi Enkripsi Data Dengan Algoritma Vigenere Chiper, 2012.

[4] S. Singh, The Code Book - The Science of Secrecy From Ancient Egypt To Quantum Cryptography, Anchor : Paperback, 2000 .

[5] Dony Ariyus, 2006, Kriptografi: Keamanan Data dan Komunikasi, Graha Ilmu, Yogyakarta

[6] Dauglas Stinson, 1995, Cryptography: Theory and Practice, CRC Press United States